United States District Court

Eastern District of Michigan

Southern Division

Jesse R. Enjaian, Plaintiff, v. **University of Michigan President Mark S. Schlissel**, and **Bernard C. Mundt II**, and **José A. Dorta**, and **Renée J.S. Schomp**, Defendants.	Case No.: **2:14-CV-13297** Judge: **Robert H. Cleland** Magistrate Judge: **Steven R. Whalen** **Claims of unconstitutionality**

First Amended Complaint for relief under 42 U.S.C. § 1983, 18 U.S.C. § 1030, MCL 600.2911, Michigan common law intentional infliction of emotional distress, Michigan common law defamation.

NATURE OF CASE

1. Our academic system and criminal justice system depends upon the integrity of campus law enforcement officials – especially when those officials are solely employed for the special purpose of protecting the interests of their employer and its college campus, preempting local law enforcement who have virtually no vested interest in the quasi-public activities of the campus or the private interests of its current officials. When campus police transgress clear ethical boundaries they become tantamount to private security, under the guise of public official, for even the private interests advanced at a public university which has no place in the lauded bastion of civil rights at the University of Michigan.

2. This case stems from two of the most serious forms of police misconduct: the misrepresentation of an affidavit to wrongfully obtain judicially authorized, facial probable cause to conduct a search and seizure of a computer and the willful disregard of the lack of objective probable cause for the purpose of conducting a computer fishing expedition. Almost 100 years ago, Justice Brandeis vehemently protested as the law struggled with the new concept of wiretapping[1], for then novel technology (the "telephone"), that "[o]ur government... teaches the whole people by its example. If the government becomes the lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy." Both Bernard C. Mundt II and José A. Dorta never believed I was stalking Renée J.S. Schomp over two emails sent to the entirety of the University of Michigan Law School and, they only wanted to harass, subdue, and force maintenance of the status quo, at the direction of University of Michigan Law

[1] *Olmstead v. United States*, 277 U.S. 438 (1928) (overruled by *Katz v. United States*, 389 U.S. 347 (1967)).

School Dean of Students David H. Baum for starting a competing student government at the Law School. And they abused the law to do so. When José A. Dorta became angered that I would not provide access to my encrypted data without judicial order he retaliated by using methods that no objectively reasonable officer would use – and in violation of clearly established Sixth Circuit law – to search my computer for the sole purposes of delay, harassment, and invasion of privacy.

JURISDICTION AND VENUE

3. This Court has federal-question jurisdiction over the claims arising under 42 U.S.C. § 1983 and 18 U.S.C. § 1030 under 28 U.S.C. § 1331.

4. This Court has supplemental jurisdiction over the claims arising under Michigan state law under 28 U.S.C. § 1367.

5. Venue is proper under 28 U.S.C. § 1391(b) because all the events giving rise to this action occurred in the Eastern District of Michigan.

6. There is an actual controversy between Plaintiff and Defendants within the meaning of the Declaratory Judgment Act, 28 U.S.C. §§ 2201, 2202, and Federal Rule of Civil Procedure 57.

PARTIES

7. Plaintiff Jesse R. Enjaian is a citizen of California living at 4457 Alameda Drive, Fremont, California. During the times pertinent to this Complaint, I was a student at UMLS and living in Ann Arbor, Michigan. The agreement to receive instruction between UMLS and I was made for approximately $220,000 and was entered into, by me, in Alameda County, California.

8. Defendant University of Michigan President Mark S. Schlissel ("Schlissel") is the president of this branch of the State of Michigan with its principal place of business located at 503 Thompson Street, Ann Arbor, Michigan. Defendant Mark S. Schlissel is sued only in his

official capacity.

9. Defendant Bernard C. Mundt II is a citizen of Michigan and works full-time at U-M for its campus police at 503 Thompson Street, Ann Arbor, Michigan as a duly appointed and acting police officer. As such, he acted under color of law pursuant to the statutes, ordinances, regulations, policies, and customs of the University of Michigan and the State of Michigan. During the times pertinent to this Complaint, he was permanently domiciled in Michigan and working full-time at the U-M Department of Public Safety in Ann Arbor, Michigan. Defendant Bernard C. Mundt II is sued in both his official and unofficial capacity.

10. Defendant José A. Dorta is a citizen of Michigan and works full-time at U-M for its campus police at 503 Thompson Street, Ann Arbor, Michigan as a duly appointed and acting police officer. As such, he acted under color of law pursuant to the statutes, ordinances, regulations, policies, and customs of the University of Michigan and the State of Michigan. During the times pertinent to this Complaint, he was permanently domiciled in Michigan and working full-time at the U-M Department of Public Safety in Ann Arbor, Michigan. Defendant José A. Dorta is sued in both his official and unofficial capacity.

11. Defendant Renée J.S. Schomp is a citizen of California living at 501 Sandretto Drive, Sebastopol, California. During the times pertinent to this Complaint, Schomp was a student at UMLS and lived in Ann Arbor, Michigan. Schomp also entered into an agreement to receive instruction from UMLS, and it was made for approximately $220,000.

FACTUAL ALLEGATIONS

12. During our first year of law school, Renée J.S. Schomp (“Schomp”) and I were classmates at the University of Michigan Law School (“UMLS”). We shared an identical set of

classes during our first year which also means that we sat in the same room and had casual conversations together amongst classmates throughout an entire school year from the early morning to the early evening. We also, often, shared lunch benches with mutual friends and engaged in casual conversation during lunch because both of us held leases with UMLS to stay in its dormitory and eat at its lunch hall.

13. During our second year of law school, Schomp began to strongly dislike me for unexplained reasons. Schomp began defaming me (i.e., gossip based on untrue factual assertions) and expressing her strong dislike of me to other students and some that happened to also be mutual friends.

14. At the time, I was not aware that Schomp's ex-girlfriend ("CC") and Schomp were in a "casual relationship." During the times relevant to this Complaint, Schomp was not openly homosexual or bisexual, rather, she had openly just ended a relationship with a longtime boyfriend prior to entering UMLS. CC and I were mutual friends, and we are still friends to this day. CC ended her relationship with Schomp as a result of this search and seizure because she believed Schomp was malicious and dishonest in her various reports against me to investigative agencies within the University of Michigan ("U-M"), particularly the then existing Department of Public Safety. Ex. 14.

15. I sent two text messages to CC that pain me every time I read them. *They are mean, immature, and obviously written by someone who was unhappy*. However, they do not give rise to probable cause for stalking or any other crime. On November 21, 2011, I wrote to CC, in a cell phone text message ("SMS"), that "I hope she [Schomp] likes deep dark pits of depression because I'm a petty bastard" and"[n]ot that serious. Just enough to make her feel crappy." These

SMS messages were part of a larger conversation, at the time, between CC and I that mitigates[2] the inference of intent to do something from these two SMS messages.

16. One night, Schomp read the SMS messages from CC's phone then several days later Schomp requested from CC that she email her a transcription of the SMS text messages. CC did so. Bernard C. Mundt II ("Mundt") intentionally, knowingly or recklessly removed the dates and times associated with the SMS message transcription before submitting them to the magistrate during the independent review for probable cause for the sole purpose of misrepresenting the affidavit to the magistrate. Ex. 1. Specifically, Mundt willfully removed the dates and times to *mislead the magistrate into believing that the SMS messages were sent after* Schomp expressly told me, on November 22, 2011, not to have any further communication with her. No reasonable officer would have done so because they were not; the messages were sent the day before on November 21, 2011.

17. Schomp expressed her right to remain free from individualized communication from me on November 22, 2011. I understood this as a clear and plain statement to stop communicating with Schomp, and that is was what I intended to do and did. Additionally, CC warned me, via SMS messages, that Schomp was going to go to the police if I continued to bother her and I acknowledged this, via SMS, when I expressed that I felt Schomp was

---

[2] On November 23, 2011, the day after I was informed by Schomp to cease communication with her, the following exchange of SMS messages, between the only other witness than Schomp that Mundt relied upon, were transmitted in response to my admission to CC (see ¶ 6) that Schomp informed me to cease communication: "[i]nteresting…what are you gonna do about it?" and my immediate response "Nada…She wants to entrap me in some harassment claim with the fem-nazis, so no I will not message her again…" all on November 23, 2011. Both Mundt and Schomp were aware of these because they were provided in the transcription (see ¶ 6) that Mundt relied upon.

attempting to "entrap" me in a harassment claim.

18. On December 9, 2011, using features designed explicitly for group email communication on the U-M website for its students, I started a functional parody of a law school administered student group, the Law Open Listserve ("LawOpen"), called the Law Closed Listserv ("LawClosed"). When one member of UMLS sends an email to lawopen@umich.edu, the UMLS computer servers then forward this email to every law student at UMLS. LawOpen is typically used to buy or sell things that are common among the population at UMLS (e.g., old casebooks, outlines, treatises, housing, etc.). LawClosed functioned identically: an email sent by a member of UMLS to lawclosed@umich.edu would also be forwarded, by features for group communication over email made available to U-M students via the U-M student website, to every member of UMLS. The distinguishing feature of LawClosed is that it was an unmoderated forum without the ability to limit access to UMLS students by other UMLS students. Ex. 13.

19. Schomp was aware of and regularly used LawOpen. Schomp was also aware that LawClosed was similar or identical in nature to LawOpen, specifically, she was aware that messages sent to lawclosed@umich.edu were automatically forwarded to the entirety of UMLS. Ex. 14.

20. The same day, Schomp reported to Mundt that she "feels frightened and harassedby [sic] receiving two e-mail messages from Enjaian." The first email, Ex. 3, was my "introduction" to LawClosed which was used to demonstrate its existence to the entirety of UMLS. The second email, Ex. 4, was my personal use of LawClosed which was used to sell an old casebook, and I actually sold it later that week as a result of that email. Schomp intentionally and knowingly told Mundt she felt frightened and "harassed" by both the introduction email and the offer to sell a

casebook for the sole purpose of misleading the magistrate's independent evaluation for probable cause. As a result of Schomp's malicious report and Mundt's wrongful misrepresentation, the property described in Exhibit 1 was seized until U-M returned it to me early 2013. UMLS shutdown the parody listserv, lawclosed@umich.edu, the morning of December 10, 2011. Ex. 13.

21. Near December 9, 2011, Schomp also filed a complaint with the University of Michigan Office of Student Conflict Resolution ("OSCR") alleging an identical claim of stalking. This complaint resulted in an administrative investigation which concluded that I had not stalked Schomp pursuant to U-M student rules, and I graduated with my J.D. in May, 2013 from UMLS without any disciplinary action from U-M. Ex. 11.

22. Schomp lied to both U-M and José A. Dorta ("Dorta") asserting I was physically violent towards other students and that I possessed a firearm with the intent to commit a mass-murder at U-M. Schomp learned that no charges had been filed because no crime had been committed. After seizing and searching my computer and other equipment, neither Mundt nor Dorta found evidence to support prosecution of stalking or any other crime. Schomp then decided to take the law into her own hands. She began interviewing students about me, including my ex-girlfriend (who provided a written declaration in my support to OSCR). Schomp did not agree with the evidence she was provided with from other students, so she began fabricating evidence. She did this by asserting that other students made the claim while she merely was reporting what they said. Apparently her lies were credible because the U-M Dean of Students – based on no other evidence than Schomp's libelous email – interviewed me for the sole purpose of assessing whether I was going to commit an act of violence at U-M. Ex. 15.

23. Schomp submitted her falsified investigation, at the encouragement of UMLS Dean of

Students David H. Baum ("Baum"), to both OSCR and Dorta, maliciously or intentionally and knowingly, to interfere with my education at UMLS by wrongful criminal or UMLS student rule conviction, discipline or investigatory interference. Schomp was aware that either would likely delay or prevent my graduation or otherwise interfere with my education from UMLS.

CLAIMS FOR RELIEF

Claim I*: Malicious, intentional and knowing, or reckless misrepresentation of the affidavit in support of the search warrant in violation of the Fourth and Fourteenth Amendments and Article I, §§ 11 and 17 of the Constitution of Michigan, against Mundt under 42. U.S.C. § 1983.*

24. Claim I fully incorporates the contents and allegations of paragraphs 12-23.

25. The statute of limitations for this claim has not ran, however, this claim is not barred by the statute of limitations for substantive, discovery reasons as well. The emails referenced in the warrant affidavit (Ex. 3 and 4) were only present on the computer seized by Mundt, and I did not remember them until discovery in early 2013. Registration information illustrating the recipients of the emails referenced in the affidavit for the *LawClosed*, *infra*, list serv was also only present on the computer seized by Mundt. Likewise, the text messages referenced in the warrant affidavit, *infra*, were only present on the cell phone seized by Mundt, and I did not remember them until discovery via FOIA in early 2013. Defs.' Answer, p. 3 ¶ 7, 2:14-CV-13297, October 13, 2014, ECF No. 11. As a result of the lengthy seizure, I did not discover Mundt's true misrepresentations until the return of my property. Upon return of my property, I discovered Mundt's intent to misrepresent the affidavit contained in his narrative report of his investigation

that he wrote in early 2013.

26. Mundt's misrepresentations were done at the behest of UMLS exploiting the cronyism at the then existing Department of Public Safety. UMLS makes money hand-over-fist selling its image as a "premier law school"[3] to the legally untrained and neophyte. Unfortunately, image often lacks substance. Like any other ABA-accredited law school, the education at UMLS was quite standardized, and without the charlatanic image marketing itself as the tower for the wizards of the legal realm they'd soon lose their "Top 10" standing that they grasp to for the associated profit dispersed in the average $200,000-$300,000 professorship salary at UMLS. Mundt was acting at the direction of UMLS to silence the growing dissent amongst students at UMLS about staff and non-teaching faculty's fraudulent misrepresentations to potential and current students. The parallel student government I created only threatened UMLS's image (and, hence, profit) and could not possibly support a true suspicion of stalking.

27. The Fourth and Fourteenth Amendments to the Constitution – as well as Michigan's ratification of such values in its state constitution – protect against both unreasonable searches and seizures and the arbitrary denial of life, liberty, and property. These bedrock principles emerged from the Federalist era and *they will survive the Internet era*.

28. Mundt misrepresented his affidavit to materially and falsely imply probable cause existed when, under the objective facts, it did not. This was done in violation of clearly established law and no reasonable officer would've sworn the following:

29. Mundt placed ¶ D after ¶ C to imply that the communication referenced in ¶ D happened subsequent in time to ¶ C. Ex. 1. In fact, the communications referenced in ¶ D was

[3] Defs.' Mot. for Sanctions, p. 4 ¶ A, 2:13-CV-13907, January 17, 2014, ECF No. 37.

sent to CC on November 21, 2011 prior to Schomp's express desire that I cease all communication with her on November 22, 2011. Ex. 2.

30. Mundt removed the date and time from the SMS messages referenced in ¶¶ D and E while leaving them in ¶¶ B, C and F to mislead the magistrate into interpreting Mundt's affidavit as stating facts that support I was willfully continuing on a course of conduct to communicate with Schomp.

31. Mundt used the date of December 9, 2011 (the date that Schomp forwarded the transcriptions to Mundt) instead of the date of transmission of the communications to imply that ¶ D happened subsequent in time to ¶ C to cause the magistrate to misinterpret Mundt's affiance as stating facts that I was willfully continuing on a course of conduct to communicate with Schomp.

32. Mundt swore that ¶ F supported probable cause for stalking while he was aware it was sent to the entirety of UMLS for the sole purpose of misleading the magistrate into interpreting his affiance as stating facts that I directed those emails towards Schomp. No reasonable officer would've believed Schomp was truly frightened by either of these emails, but Mundt submitted his affirmation for the sole purpose of misleading the magistrate into misinterpreting his affiance as stating facts that I was willfully continuing on a course of conduct to communicate with Schomp. Mundt was also aware of the contents of each email, prior to seeking the warrant, and that the second email was an offer to sell a book. Ex. 3 and 4. Mundt omitted a description of the second email for the sole purpose of misleading the magistrate into interpreting his affidavit as stating facts that both emails were directed towards Schomp, fulfilling the two contact requirement of the plain text of the stalking statute in Michigan.

33. Mundt omitted SMS messages that indicate my intent to *do nothing* in his affidavit to the magistrate for the sole purpose of misleading the magistrate into misinterpreting Mundt's affiance as stating facts that I was willfully continuing on a course of conduct to communicate with Schomp.

34. Paragraph H of the search warrant does nothing to assist in determining probable cause. Ex. 1, ¶ H.

Claim II*: Malicious, intentional and knowing, or reckless restriction of protected speech under the First and Fourteenth Amendments and Article I, §§ 5 and 17 of the Constitution of Michigan, against Mundt under 42 U.S.C. § 1983.*

35. Claim II fully incorporates the contents and allegations of paragraphs 12-23.

36. The statute of limitations for this claim has not ran, however, this claim is not barred by the statute of limitations for substantive, discovery reasons as well. The emails referenced in the warrant affidavit (Ex. 3 and 4) were only present on the computer seized by Mundt, and I did not remember them until discovery in early 2013. Registration information illustrating the recipients of the emails referenced in the affidavit for the *LawClosed*, *infra*, list serv was also only present on the computer seized by Mundt. Likewise, the text messages referenced in the warrant affidavit, *infra*, were only present on the cell phone seized by Mundt, and I did not remember them until discovery in early 2013. As a result of the lengthy seizure, I did not discover Mundt's true misrepresentations until the return of my property. Upon return of my property, I discovered Mundt's intent to misrepresent the affidavit contained in his narrative report of his investigation that he wrote in early 2013. Additionally, I did not discover evidence of Mundt's intent to misrepresent the affidavit contained in Exhibit 12 until early 2013 via FOIA.

37. Our society relies upon equality in its diversity governed by the immutable rules of the Constitution and not thuggish contempt for those we disagree with. Whether it be the exercise of religious freedom or political speech, the First Amendment of the Constitution and the associated section of the Constitution of Michigan protect fundamental, individual rights to speech. Including nonviolent, legal sedition and subversion and speech done for the purpose of making a profit.

38. Mundt asserted in his affidavit that the two emails I sent to lawclosed@umich.edu constituted stalking under state law in Michigan. Ex. 1, ¶ F.

39. Mundt was aware, prior to seeking the warrant, that lawclosed@umich.edu was not simply a "large group of UofM Law School students," rather, it consisted of the entirety of UMLS. Ex. 1 and 14.

40. Mundt was aware, prior to seeking the warrant, that the second email, Ex. 4, was an offer to sell a course casebook to the entirety of UMLS.

41. The plain text of the stalking statute in Michigan exempts speech that serves a legitimate purpose or is constitutionally protected. Both of my emails served a legitimate purpose: the first to introduce the existence of LawClosed to UMLS and the second to sell a textbook. Ex. 3 and 4. The second email was identical in form and nature to other offers to sell textbooks that are, to this day, sent through LawOpen. Both of my emails are also constitutionally protected due to the sheer volume of recipients (i.e., the entirety of UMLS) and the complete deficiency of any indicia that the emails were directed towards Schomp. Ex. 13.

42. Based upon this information, Mundt wrongfully misrepresented and submitted the exercise of my First Amendment rights for the support of probable cause for stalking. Mundt did

this to restrain my dissent, of the "Big Law" career-path all but mandated by UMLS, through the rebellious LawClosed listserv; the LawClosed listserv was shutdown the morning after the execution of the night search warrant (i.e., less than twelve hours later) at the request of Baum. Ex. 12.

Claim III*: A declaration finding the search warrant lacks probable cause and is unconstitutionally over broad in violation of the Fourth Amendment and Article I, § 11 of the Constitution of Michigan, under 42 U.S.C. § 1983.*

43. Claim III fully incorporates the contents and allegations of paragraphs 12-23 and *Claims I-II* and *IV-V*.

44. There is an actual controversy because the statute of limitations for criminal stalking runs and the Defendants can re-request the filing of charges anytime prior to the expiration of that limitation. Dorta retains the data and other evidence gathered from his investigation and can re-request filing even now. Ex. 17.

45. The warrant sought and obtained by Mundt lacks probable cause. By striking out the paragraphs in Mundt's affidavit that (1) do nothing to assist determining probable cause, (2) maliciously, intentionally and knowingly, or recklessly misrepresent facts to the magistrate, and (3) maliciously, intentionally and knowingly, or recklessly rely on unreasonable information, Exhibit 2 clearly demonstrates the facial lack of probable cause that Mundt circumvented for the purpose of misleading the magistrate.

46. The warrant sought and obtained by Mundt lacks particularity. The warrant was also over broad and authorized search of the entirety of my computer, including files wholly unrelated to stalking, and the warrant did not describe with particularity what evidence was sought (i.e., the

warrant did not restrict the search to evidence of stalking). The warrant authorized the search and seizure of no less than "[a]ll computer equipment, information storage devices and cell phones as well as records or documents* that are located at the above and there contents." Ex. 1. The warrant did not specify that these items were to be searched only for evidence of stalking, hence, this language expressly authorizes searching my photo library, music library, and many other files with no plausible relation to stalking for which I retain privacy rights.

Claim IV*: Unreasonable execution of search violating the Fourth and Fourteenth Amendments and Article I, §§ 11 and 17 of the Constitution of Michigan, against Dorta under 42 U.S.C. § 1983.*

47. Claim IV fully incorporates the contents and allegations of paragraphs 12-23 and *Claim V.*

48. Both the Fourth and Fourteenth Amendments to the Constitution – and the associated ratification of those values in the Constitution of Michigan – protect against unreasonable searches and seizures and arbitrary denials of life, liberty, and property. Dorta used two distinct and unreasonable search methodologies while executing his search of my computer which caused the unreasonable 446 day delay to return my seized property. It is clearly established law within the Sixth Circuit that a computer search must be tailored, in some fashion, to particularity. Dorta's search maliciously, intentionally and knowingly, or recklessly was conducted, for a large part of the 446 day search, using methods which have been scientifically proven incapable of yielding evidence and that any reasonable officer would know is hyperbolic quackery. Dorta did this to simply delay and harass in response to what he perceived as my attempts at "pressuring" the then existing Department of Public Safety into timely returning my property. Ex. 9. These

methodologies had no reasonable chance of successfully culling evidence of stalking, and when encroaching upon civil liberties, reasonableness is the first and the last principle.

49. Dorta's investigation was unreasonably executed, *in part*, because he did not purchase the hardware and software necessary to search my cell phone, and what else may be shown at trial was at least recklessly delayed, until immediately after my first lawsuit, approximately sometime in September, 2012. While there are no constitutional *time* limits for execution of a search, there are limits on how a search is executed: as is the case here, delaying a search, without good faith cause (i.e., simply not conducting the search which is what Dorta alleges occurred), for nine months is an unreasonable method of execution of a search warrant, denying me my property without any attempt at due process, and the reasonableness of Dorta's inaction must be determined by the jury. Ex. 17, p.4 ("on 9/25/12 after some updates..."). Surely the Constitution protects against wrongful and unreasonable, procedural foot-dragging at the expense of civil rights.

50. Dorta alleges the *other* unreasonable delay was primarily because his attempt to "brute-force attack"[4] my encrypted data was a slow process that required a long period of time to complete. Ex. 18. Dorta admits that he had 2-3 personal computers attempting to brute-force decrypt my data since shortly after the seizure on December 9th, 2011. *Id*.

51. My encrypted data was encrypted with the Advanced Encryption Standard ("AES") published by the United States National Institute of Standards and Technology in 256-bit chained block cipher mode using fourteen rounds ("AES CBC14"). This is also the default setting for the

[4] "Password cracking" is a misleading and pedestrian definition with its origins likely from Hollywood, California. It describes nothing more than the proposition "attempting to access data protected by a password without knowledge of the actual password."

now defunct software package TrueCrypt™ version 7.1a which is what was installed on my laptop and what Dorta admits he believed was in use by me. *Id*.

52. "Brute-force attacks" are a subject matter of scientific fact. Brute-force techniques are also scientifically, demonstrably impossible to use to gain access to data encrypted with AES CBC14 within less than substantially more than several million years with any statistical significance[5] or measurable probability using the modern, commercially available computers available to U-M.

A general description of the immunity to brute-force cryptanalysis of modern cryptographic ciphers.

53. The following paragraphs *generally* explain how cryptography works so that the previous paragraph is not merely conclusive to a reader without any prior knowledge because this is a fundamental requirement for *understanding* how Dorta's "brute-force attack" was, specifically, an unreasonable execution of the search warrant:

54. At its most fundamental basis, *cryptography* is any method of hiding the true meaning of a written message, or, in the case of computers, to hide the true meaning of data. Cryptography fundamentally consists of two processes: *encryption* to hide the message and *decryption* to unhide the message. These methods, combined, are called a *cipher* and almost certainly there are

[5] *Statistical significance* is the term used by mathematicians to divide the "probability" of something between possible and impossible in terms subjective to humans versus objective mathematical terms that can result in outcomes never before witnessed by humans. For example, Gallup, Inc. asserts President Barack H. Obama's "job approval" by the voting adult population of *all 313.9 million people* in the United States is exactly 40% today with a statistical significance of 5%. In other words, there is a 5% measure of probability that more or less than 40% of the adult population asserts "job approval" for the President today. In medical research, a statistical significance of 5% is far too large a *margin of error* and much smaller values are necessary to ensure reasonable patient safety.

more ciphers in existence than are publicly known because there are very few restrictions on what defines a cipher.

55. Cryptography is everywhere in our society; without it we could not have commerce on the Internet or even PACER. Cryptography is nothing new. It's existed before computers, and the use of cryptography dates as far back as the Egyptians when it was used to hide the true meaning of hieroglyphs. In today's workplace, it's professional negligence to store private client information unencrypted[6] on a computer and results in numerous class action lawsuits for stolen SSNs and credit card information each year[7].

56. The first use of modern cryptography was by Julius Caesar and, nowadays, cereal-box prize "decoder rings." This cipher is *not* constructed with rigorous mathematics (and it is materially similar to the Enigma cipher used by Nazi-Germany): letters in the Latin alphabet are exchanged with others, and, therefore, to decrypt an encrypted message you must know which letters are exchanged with other letters. For example, the encrypted message "KD MCSAL" is encrypted using the following *parameters*: the subset of the English alphabet {K↔H, D↔I, M↔J, C↔U, S↔D, A↔G, L↔E} which decrypts "KD MCSAL" to "HI JUDGE."

57. Of course, Caesar's cipher is quite easy to decipher, using computers, without any

---

[6] In fact, the content of one my encrypted volumes, "mic.tc," was just this. It was confidential client information from my participation in the **M**ichigan **I**nnocence **C**linic at UMLS, and it was encrypted with the now defunct software package **T**rue**C**rypt™ version 7.1a.

[7] For example, infamously, last month Home Depot® customers fell victim to the largest number of credit cards stolen from a company's computer payment systems with 55 million unique cards (that's about 23% of the adult population of the United States) lost to criminals, likely, from across the world solely because of storing the card numbers both electronically and unencrypted. Less than a month later, a class action for negligence was brought in the United States District Court for the Northern District of Illinois.

knowledge of the parameters of the cipher. Just have a computer "brute-force" try every exchange, or *permutation*, of letters until words from the dictionary are found (i.e., "HI" or "JUDGE"). In fact, there are a relatively small, finite number of exchanges[8] which are easily computable with modern, consumer computers. And this doesn't even account for patterns in English grammar and usage.

58. "Brute-force" techniques to decipher data from a known cipher without any knowledge of its parameters is part of a larger class of methods called *cryptanalysis*. Many methods of cryptanalysis can be quite effective, however, there are no publicly known methods of cryptanalysis for AES CBC14 other than "brute-force."

59. "Brute-force," like cipher, is loosely defined. It can mean trying every possible parameter until the message is un-hidden. All modern ciphers, including AES CBC14, are specifically designed to be statistically immune to brute-force cryptanalysis. In other words, the probability of its success after 446 days of trying is still insubstantial relative to the human life-span (i.e., it's unfathomably lower than even the "odds" of winning Michigan's state MegaMillions™ or PowerBall™ lottery – several years in a row or, in other words, three times every 1,625,183,253,179,503,440,124,358,656 times played there will be a statistically significant likelihoods of winning).

60. Unlike Caesar's cipher, AES CBC14 cannot be deciphered by brute-force within a reasonable amount of time. If you're thinking that it's merely a question of the number of

---

[8] i.e., $26! = 403,291,461,126,605,635,584,000,000$ or, in English, 403 million billion billion exchanges. Contrast this with the computer you're likely reading this on: the latest consumer microprocessors from Intel, Inc. and Advanced Micro Devices, Inc. (AMD) can calculate almost 3.2 billion exchanges per second.

computers or time or that a shot-in-the-dark can still hit its target then you do not appreciate the unfathomable scale of the mathematical and philosophical concept of infinity (indeed, most neuro-psychologists and mathematicians don't believe the human mind is capable of even visualizing a quantity so largely foreign to our existence[9]) that renders such an effort statistically insignificant and probabilistically immeasurable. Imagine[10] the following cipher. Let numbers represent alphabet letters (i.e., {A↔1, B↔2,...,Z↔26}), then we can encrypt a message using the modulus operator (i.e., the remainder in division) and finding congruencies[11] with other numbers in $\mathbb{N}$ (the natural numbers; that is, zero and the positive integers [0, 1, 2, 3,..., ∞)). We can then choose prime a number to encrypt the letter "D" with: $4 \equiv 4 \times 102{,}763^{1{,}234} \pmod{102{,}763}$.[12]

---

[9] Mathematician Georg Cantor, the inventor of set theory, proved there are two sizes to the mathematical concept of infinity. Cantor distinguished the two infinities by proving that a set composed of the integers is strikingly smaller than another set that must exist (e.g., the real numbers). In other words, there is a strikingly larger infinite number of real numbers within the interval [0, 1] (e.g., 0.1, 0.11, 0.111, 0.1111, etc.) than there are integers in the infinite set [0, 1, 2, 3,..., ∞). This, of course, is quite distinct from the tautological, false, and uninspired proposition that ∞ is less than ∞ + 1.

[10] This is not a specific pleading of fact for plausible relief under *Iqbal*, rather, it is an explanation for use in understanding that the following paragraphs in this claim assert facts for plausible relief. Indeed, the cipher used in this hypothetical is not even used in AES; it is merely a device for education.

[11] Congruencies are often analogized to the face of an analog wall clock. For example, $3{:}00 \equiv 15{:}00$ and $0{:}00 \equiv 12{:}00$ because the hands repeat themselves every twelve hours. In arithmetic, this means that $12\overline{)3} \equiv 12\overline{)15}$ because, in both cases, the remainder is 3. Formally, this is written as $3 \equiv 15 \pmod{12}$.

[12] The decrypted message is 4 ("D") while the encrypted message is 102,763 to the power of 1,234 times 4 – a number with 6,186 digits.

Divide either side by the modulus and you end up with 4 (or "D").[13] Hopefully it's clear that without knowing 102,763 (because this number is prime, no other number can satisfy this congruence) *it takes a significant amount of calculations before stumbling upon the right-hand side's congruence with 4* (i.e., if you sequentially tried moduli from [1, 2, 3,..., 102763] on the right-hand side of the congruence until you brute-force divide to "D"). What this trivial, epistemological example demonstrates to this Court is that picking a sufficiently large and hard-to-guess prime modulus creates a striking difference in complexity of calculations (and, hence, time due to the finite rate of calculations) between encrypting and brute-force cryptanalysis. *Pick a prime modulus so large that even all the computers in the world working together can't try all the different parameters of the cipher within several millions years*. And this is the foundation of why modern cryptography is immune to brute-force cryptanalysis. Modern encryption, *by construction*, can occur within a relatively short amount of time while brute-force cryptanalysis, also *by construction*, takes longer in time than humans have existed on earth even when theoretically using all the computers that presently exist together[14] with any statistical

---

[13] This idea was first proposed by Ronald Rivest, PhD, a computer scientist from Stanford University, in 1983 while researching at the Massachusetts Institute of Technology. Ex. 8. Undoubtedly, this Court has already used several implementations of his various cryptographic inventions today without even being aware of it.

[14] Bruce Schneier is a leading industry expert in the field of cryptography. He's been featured in *Wired Magazine* and authored the seminal book *Applied Cryptography* (2d ed. 1996). Schneier, explaining the complexity of cryptanalysis on a class of ciphers that includes AES found: "Calculating the complexity of a brute-force attack is easy. If the key is 8 bits long, there are 2^8, or 256, possible keys. Therefore, it will take 256 attempts to find the correct key, with a 50 percent chance of finding the key after half of the attempts. If the key is 56 bits long, then there are 2^{56} possible keys. Assuming a supercomputer can try a million keys a second, it will take 2,285 years to find the correct key. If the key is 64 bits long, then it will take the same supercomputer about 585,000 years to find the correct key among the 2^{64} possible keys. If the key is 128 bits long, it will take 10^{25} years." Bruce Schneier, *Applied Cryptography* 175 (2d ed.

significance. Ex. 7.

A specific description of how Dorta's attempted cryptanalysis of my AES CBC14 encrypted data was also immune to "brute-force" methods.

61. Dorta, *specifically*, attempted to brute-force decrypt my encrypted volumes by *guessing* the password on a sequential basis. That is, the first password tried was "a," the second "aa," the third "aaa," and so on until a maximum password length, arbitrarily chosen by Dorta was reached (e.g., "aaaaaaaaaaaaaaaaaaaaaaa") then the sequence began permutating with the remainder of possible password values. That is, the first permutation was "b," the second "ba," the third, "ab," and so on until the arbitrary maximum was again reached with "bbbbbbbbbbbbbbbbbbbbbbb." It should be evident that, given the previous hypothetical about the complexity of calculations and the time-dependent rate of calculations that brute-force cannot succeed within a reasonable amount of time against AES CBC14 because the time it takes to brute-force decrypt a single letter from AES encrypted data is, *by construction*, longer than humans have existed. Ex. 5, p. 10; Ex. 6; Ex. 7. This specific method employed by Dorta could not have been successful within any reasonable amount of time at any statistical significance because the specific method of brute-force employed by Dorta is less exhaustive with no more likelihood of successfully guessing the "password" than the theoretical and exhaustive attempt at brute-force cryptanalysis of AES CBC14 through much longer than several million years of computationally guessing (e.g., iteratively through every distinct possibility). In other words, only buying lottery tickets with your "lucky" numbers doesn't change your odds one bit.

62. Additionally, while Dorta's search never could've succeeded as a matter of statistical

---

1996).

insignificance it also was destined – even when theoretically operating through eternity – to fail because it was conducting a “brute-force attack” against “Ripe-160 encryption” which is, of course, not AES CBC14. Ex. 18, p. 11 ¶ 10. Brute-force is a process of exhaustively attempting to decrypt encrypted data with all possible permutations of the parameters used in the cipher, hence, brute-force methods are specific to a cipher. Without knowing how to conduct a search then no possible search can occur. For example, the famous quote by abolitionist and civil rights activist W.E.B. Du Bois "*When you have mastered numbers, you will in fact no longer be reading numbers, any more than you read words when reading books. You will be reading meanings.*" when encrypted with Caesar’s cipher using a parameter of “shifting” the letters of the alphabet, lined in a row, to the left by 13 letters while retaining all 26 letters is “Jura lbh unir znfgrerq ahzoref, lbh jvyy va snpg ab ybatre or ernqvat ahzoref, nal zber guna lbh ernq jbeqf jura ernqvat obbxf. Lbh jvyy or ernqvat zrnavatf.” Now, when encrypted with AES in 128-bit chained block cipher mode using thirteen rounds with the key-parameter (synonymous but methodologically distinct from what this Court refers to as “password”) “password” the encrypted quote is

“14nsBYOBwjBv6PKuKS0m2WKjgzy6x4ljVlHkEFJfnkBjbiUSZjtAJeeLsRZvRd0GFyif7Phmv20/Zith002wVZCFImBce+/BVV3CLgT2yac1ty6mwAkvUxzvXcNJygFfjha24/7xkIydj9khuqQrEiWjJo/YV37G3Ay5knFjDeYftvV32Ne4x3aTQNPXT/MJJ6ZpibvnW9J9AIXbQn3UrtSzrqDD+fVACbc8f+RS7Y+2v2Z+3Cxo527iCbqyQMfNrzUOeYhzNRUHTo9AoamMfRq1HW0cXgXz/NuAKia8jGc=” which is clearly not produced using similar methods to Caesar’s cipher. Any attempt to use the same methodologies to “work-backwards” from the quote encrypted with Ceasar’s cipher with the quote encrypted with AES in 128-bit chained block cipher mode using

thirteen rounds is merely irrational.

63. For emphasis, I re-allege the paragraphs of this claim: *brute-force cryptanalysis of AES CBC14 encrypted data is an unreasonable method of execution of a computer search warrant because it cannot be used to do what it purports against AES CBC14 within less than substantially more than several million years*, and cryptanalysis cannot be performed without knowledge of the cipher in use (i.e., the brute-force method for Caesar's cipher cannot be used with our hypothetical modular cipher or vice verse – it should be clear it is irrational to attempt so) because brute-force methods are specific to each cipher.

Conclusion that the Fourth and Fourteenth amendments protect AES CBC14 encrypted data from bogus brute-force cryptanalysis.

64. Brute-force cryptanalysis of AES CBC14 is no more effective a tool for discovering evidence than a divining rod for finding a body, psychic visions accusing a suspect, or any other quackery. Without constitutional protections against bogus methodologies for discovering evidence there is no efficacy from the constitutional protections originally envisioned hundreds of years ago before computers were invented. There are an infinite number of ways to do something wrong (for instance, this is my *third* attempt at adjudication of this matter) and without some reasonable limitation, it's easy to imagine false methodology after false methodology asserted as justification for retaining the products of a seizure. The highly commercialized defense and security industry can sell you whatever you need, neatly packaged in a magic bottle, for a price; but our constitutional protections, of course, place no pressure on the completion of legitimately lengthy investigations.

Claim V*: Relief for access, without authorization or in excess of authorization, of a protected computer while conducting an unreasonable search and seizure, outside the scope of good faith reliance upon a facially valid warrant, under the Fourth Amendment and Article I, § 11 of the Constitution of Michigan, against Dorta under 18 U.S.C. § 1030(a)(2) and 42 U.S.C. § 1983.*

65. Claim V fully incorporates the contents and allegations of paragraphs 12-23 and *Claim IV*.

66. The portion of this claim that is colored under the Computer Fraud and Abuse Act is not barred by the statute of limitations because I did not discover Dorta's search was over broad until reading his narrative report, Exhibit 17, in early 2013.

67. It is not sufficient if a warrant authorizes the search and seizure of an entire computer without requiring the search be conducted for a crime enumerated in the warrant application. A warrant that authorizes the search and seizure of an entire computer system without requiring the search be for a specific crime is so blatantly lacking in any indicia of probable cause that any reasonable officer acting under the color of the warrant would know their actions are lawless, illegal, and likely criminal.

68. Dorta's unauthorized search, outside the scope of a valid search warrant, resulted in the seizure of intellectual property and trade secrets owned by me that required over $10,000 in remedial computer repairs and forensics to investigate and fix the security procedures, implementations, and devices broken and stolen by Dorta. This was wholly due to Dorta's access of information outside the scope of objectively reasonable reliance upon the warrant.

69. The computer equipment seized by Mundt was later searched by Dorta. At no time

did I consent to search nor provide access to any of my information.

70. At all times relevant to this Complaint, the computer equipment seized was connected, through the Internet, to computers in California to perform legal research pursuant to my agreement with UMLS. At all times relevant to this Complaint, the computer was also connected to computers in California owned by Google, Inc., Yahoo!, Inc, and Facebook, Inc. to send and receive email and other electronic messages, conduct legal research, and send and receive intellectual property owned by me through the Internet.

Over breadth of execution argued from a legal, ontological perspective.

71. The warrant authorizing the search and seizure of my *entire* computer for the crime of stalking lacks any indicia of probable cause and any objectively reasonable officer would know this. Dorta admits in his narrative report that he viewed each and every image on my laptop, viewed my entire music catalog, and copied "virtual machines" all for the alleged investigation of criminal stalking; there is no reasonable argument how these items of data could lead to evidence of stalking. Ex. 18. Hence, the remainder of this claim relies upon Dorta's malicious, intentional and knowing, or reckless search and seizure disregarding the objective lack of probable cause for what was, in part, distinctly seized. *Cf. Messerschmidt v. Millender*, 565 U.S. ___ (2012) (the Court found qualified immunity applied when relying upon a warrant lacking probable cause because the officer was acting objectively reasonable). It's easy to imagine that the search could have been more limited by searching only for *evidence of stalking*, yet, clearly, Dorta's search was conducted upon the entirety of the computer (i.e., Dorta viewed each and every file contained on the computer).

72. Dorta's objectively unreasonable actions are distinct from the extension of qualified

immunity advanced by *Messerschmidt*. Here, over breadth is argued from actual, wrongful search and seizure that did not relate back to warrant application for stalking. In contrast, *Messerschmidt* may protect the over broad seizure of distinct items of evidence that are later found not to have been searched and seized with actual probable cause. In the case of computer searches, it may be reasonable to assert that, in a stalking case, the seizure of emails unrelated to stalking are within the ambit of qualified immunity because the proposition that *an unsorted mass of emails is reasonably likely to contain evidence of stalking* may be true. My argument in this claim is that Dorta searched and seized distinct data that held no apparent relation back to the four-corners of the warrant or its affidavit (see, *infra* in this claim's conclusion) and would not have been discovered in a search tailored to criminal stalking. Without some validity to my reasoning, it's hard to imagine how a computer hard drive, in its entirety, to be seized under the guise of facial probable cause (a "pretextual search warrant") could possibly be challenged as unconstitutional. *Richards*, *infra*, at 537 ("[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect"). Unlike searches incident to an arrest, the warrant process is meant to protect against wanton violations of Fourth Amendment protections by requiring *specificity* of what is to be searched and seized prior to the boots-on-the-ground (or, here, fingers-on-the-keyboard) execution of that warrant. The Sixth Circuit acknowledged this fundamental right as applied to computers in *Richards*, *infra*, which stands for this proposition: a computer search warrant must specify that the information contained within the storage devices of a computer can only be searched for evidence of a *specific crime*. Absent a search only for evidence of stalking, the execution of a search warrant for stalking has wrongfully stepped outside the boundaries of

our Constitution. *Richards*, *infra*, at 540 ("the warrants required that the communications and computer records pertain to the listed offenses").

73. *U.S. v. Richards*, set-forth the, general, governing rule for particularity challenges to computer searches: "[s]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence." 659 F.3d 527, 540 (6th Cir. 2011) (quoting *United States v. Roberts*, No. 3:08-CR-175, 2010 WL 234719, at *15 (E.D.Tenn. Jan. 14, 2010)). This rule does not address the issue, here, that the warrant lacks any indicia of probable cause to search the *entirety* of the computer – that means its express authorization to search my IRS records for non-filing as well as a substantial amount of other equally irrelevant data (see, *infra* in this claim's conclusion) – for evidence of stalking. It can easily be conceded that emails and text messages may have been reasonably over broad, in terms of realistically executing a computer search, but it's unclear how images, music files, and "virtual machines" plausibly relate to stalking which is a crime of individualized communication (and, here, via the Internet). *Richards*, 659 F.3d at 539 ("[a] generalized seizure of business documents may be justified if it is demonstrated that the government could not reasonably segregate... documents on the basis of whether or not they were likely to evidence criminal activity").

74. The court in *Richards*, when narrowing and applying its general rule, held that "[t]he scope of the warrant was restricted to a search for evidence of child pornography crimes and did not permit a free-ranging search [internal citation omitted] ('[t]he affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for

contraband... and the warrant did not authorize [ ] seizure of *every document, but of child pornography* which is a sufficiently *specific* definition to focus the search.') (citation and internal quotation marks omitted)." *Richards*, 659 F.3d at 541-542 (emphasis added). In stark contrast to this case, the warrant application – in all four pages – made no mention of stalking outside ¶ H of the affidavit (Exhibit 1) which cannot possibly be used in establishing probable cause because it is solely based upon Mundt's feelings. This warrant does not establish a nexus (or, reasonable relation) between the affidavit asserting probable cause (apparently, for no specific crime) and the description of what is to be seized: unlike *Richards* the warrant, here, describes that the computer equipment may be seized and searched in its entirety (i.e., every file on the computer system may be searched and seized) and unrelated to any specific suspicion of a crime. The description of what is to be searched and seized simply does not limit a searching officer to only look for evidence related to the crime of stalking, and, instead, it expressly authorizes a free-ranging search of the computer. Certainly, it would have been reasonable for Dorta to only search for evidence of stalking had this more specific description been incorporated into the warrant application. *Richards*, 659 F.3d at 542 ("[t]he proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation"). Apparently, Dorta relied upon this express authorization to search my computer for whatever he felt like searching for because he seized several items clearly unrelated to stalking (see, *infra* in this claim's conclusion) and these items would not have been seized in a search tailored to criminal stalking.

Over breadth of execution argued from a factual, computer science perspective.

75. The following paragraphs, *generally*, explain how data is stored on a hard drive and accessed and how Dorta, *specifically*, exceeded the scope of the warrant under Sixth Circuit law.

76. Computers almost exclusively store data in the form of "bits." A bit is simply one state or another (i.e., a bit is a boolean value). To represent information, computers form sequences of bits referred to as "bytes." Frequently, data is represented as 7-bit bytes. For example, the American Standard Code for Information Interchange defines the letter "A" as "1000001" which is *not* the base-ten number "one million one," rather, it is read "one zero zero zero zero one" because each digit represents a boolean value of one or zero in the 7-bit *list*. *This is also, physically, how data is stored on a hard drive (Fig. 1).* A hard drive is a massive sequence of ones and zeroes stored on metal with magnetic charges. Hard drives are almost identical in form to vinyl LP records from Motown: they're circular platters (or, *cylinders*) with a read head (like the needle on a record player) that can circle over the entire cylinder. But instead of the microscopic depressions on LPs the cylinders use microscopic sectors of metal that are magnetically charged and only represent one of two boolean states. The read head, when circling around the cylinder, can measure the magnetic polarity of each *sector* (i.e., a bit).

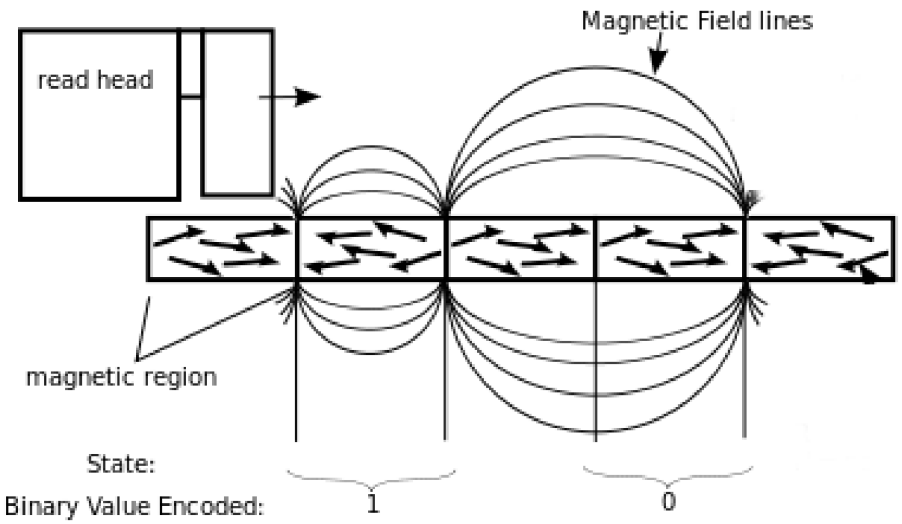

Figure 1
Five bits (or, sectors) from a circular hard drive cylinder represented linearly.

77. The Sixth Circuit has not articulated its standard for computer searches at this fundamental, mechanical level, rather, it has articulated it at the "file-system" level.

78. Because reading a sequence of binary values straight from the metal platter would quickly become intractable, all modern operating systems rely on a "file-system" which creates an abstraction from the mechanical details of the hard drive. This abstraction gave rise to the concept of "files" and "directories" as objects themselves instead of their underlying binary sequence. For instance, I am presently writing this Complaint in Corel's® WordPerfect® X5 and this file is saved as "complaint v3.wpd". The laptop that I'm writing this on stores this Complaint as a sequence of ones and zeros somewhere in its hard drive. The physical location's address (i.e., where the read head must go to begin reading the Complaint's sequence of ones and zeros) is stored at a predefined, physical location on the hard drive called the "file allocation table." In

this literal table of files[15] there is an entry for "complaint v3.wpd" with its address for its physical location on the metal platter. This file also happens to be continually uploaded through the Internet to various computers to perform an off-site backup with backup software; every time this file is uploaded, it is found not by its physical location but by searching through the file allocation table for the file named "complaint v3.wpd" then requesting the sequence located at the physical address be given to the backup software. In this abstraction, the file allocation table defines the entirety of what can be searched.[16]

79. An obvious question is how do we know that the binary sequence associated with a file name and path is what it purports to be (and, not simply that a manifesto document is

[15] For example, the following represents one possible state of this Court's computer's hard drive's file allocation table at the Eastern District of Michigan in Detroit:

File name and path for the hard drive(s) associated with S:	**Physical address on hard drive for beginning of binary sequence**
\Cleland\JUDGE'S DESK\C2 ORDERS\13-13907.ENJAIAN.MotDisqualifyMotDismissMotSanctions.jac3.wpd	Cylinder 4, Head 15, Sector 1
\Cleland\JUDGE'S DESK\C2 ORDERS\13-13907.ENJAIAN.DenyMotReconsider.jac.wpd	Cylinder 10, Head 2, Sector 5
...	...

[16] There is a corollary to this usage: what doesn't exist in the file allocation table may still exist on the hard drive. When a file is "deleted" by an operating system, it is merely removed from the file allocation table while the sequence physically remains on the hard drive. Many instances of spoilation have occurred by intentionally overwriting a sequence instead of merely removing the entry from the table, and doing so during litigation, in the Ninth Circuit, creates a presumption of spoilation. This also is a time-proven, fruitful approach to gathering evidence of heinous crimes (hence, the Sixth Circuit's abstraction to the file-system cannot be a controlling issue for particularity challenges to data on a hard drive that's *not* within the file-system).

mislabeled as “lawyer jokes.wpd”, rather, trophy pictures mislabeled as a document)? The answer computer scientists derived is to, almost exclusively, require a small portion of the beginning of a binary sequence describe what the binary sequence is, called *header* information. This is not another mere purporting of what the contents actually are, rather, the header describes the only way to interpret a binary sequence because the header is a set of rules for translation between the binary sequence and a program attempting to “open” the file. For example, removing the header from “13-13907.ENJAIAN.DenyMotReconsider.jac.wpd” removes the entire description of what the binary sequence is. In other words, you’ll be left with a binary sequence that is, on its face, indistinguishable from any other binary sequence; WordPerfect® will be unable to open a sequence without its header because it will not understand how to interpret a seemingly random binary sequence.[17]

Dorta’s use of unauthorized access to search, seize, and copy files for which no probable cause existed.

80. When Dorta initially searched my hard drive (apparently, he searched it using various and distinct methods) he attempted to power on my laptop and login to my laptop using the authentication procedures provided through the Apple OS X® Leopard® (“OSX”) operating

[17] Given the widespread use and efficacy of encryption, steganographically misrepresenting a binary sequence seems both an inept and unlikely method of hiding data. It is, however, theoretically possible that underlying binary sequences can actually contain information that is not what the file purports that may be determinable by *forensically* analyzing the entire binary sequence. But again, this is a truly asinine exception because encryption is more popular and effective at its purported goal than this awkward theoretical method; and, allowing the search of all underlying binary sequences (instead of merely the file allocation table or header information) without explicit probable cause is tantamount to an express, carte blanche authorization to search the entirety of the hard drive even for relatively insignificant misdemeanors – clearly what *Richards* was designed to prevent.

system which prevents unauthorized access without a username and password for an authorized account on my laptop. Upon failing to provide proper authentication credentials, Dorta broke into my computer by bypassing the authentication procedures from OSX and the "virtual machines" using software designed to break past those authentication procedures without proper authorization. Had there been at least objectively reasonable probable cause, Dorta would've acted within a scope of authorization to break past the OSX authentication procedures for a search under the authority of facial probable cause. But Dorta was not acting objectively reasonable, and additionally, there were also materially similar authentication procedures on my "virtual machines" – for which no plausible argument for probable cause to search and seize for stalking existed – which Dorta similarly bypassed to access the contents of the "virtual machine" (i.e., the "virtual machines" also required an authorized user and password to gain authorized access to the machine at the time of "powering on" the "virtual machines" which was also bypassed with software designed to break past those authentication procedures).

81. Once Dorta had broken into my computer, he accessed emails and work files that are intellectual property and trade secrets owned fully and partially by me. He searched, seized and copied *all* data stored on "virtual machines" on my laptop which contained private research data from business valued at over $10,000. Because Dorta lacked probable cause to search inside my "virtual machines," because they have no reasonable relation to stalking, he had no good faith authorization to access that data in full and copy it in its entirety. This is also an invasion of my privacy under Michigan common law.

82. Dorta also viewed and copied *all* of my photos and music files stored on my hard drive. My photo library is stored in a hierarchal fashion with clear labels as to its contents (i.e.,

they were stored in folders by the names of the events or people involved). The content of my photo library and the music I listen to are secrets and private subject matter that could not plausibly be used for evidence under criminal stalking. This is also an invasion of my privacy under Michigan common law.

83. During Dorta's final search he also accessed *all of my files en masse* when performing a bit-wise copy and search of my hard drive. A *bit-wise copy and search* of a hard drive is where every one and zero present on the hard drive is copied, identically in sequence, to another hard drive then searched in its entirety (i.e., every single image on my hard drive was viewed by Dorta as was confidential client information from the Michigan Innocence Clinic and my personal medical records of current prescriptions and past exam results).

84. Dorta's bit-wise copy and search of my hard drive necessarily fails any particularity requirement, rendering this part of the search outside his official capacity, because it makes no attempt to limit the search to particular items of evidence. A computer cannot simply be searched as many tangible objects are and it is subject to additional requirements that must be followed to remain within the scope of the warrant. At the very least, the Sixth Circuit requires computers to be searched for evidence of a particular crime rather than allowing the bit-wise search and seizure of everything on a computer's data storage, unless explicitly authorized by a warrant (e.g., a subsequent warrant after the initial seizure or a sufficiently detailed affidavit establishing the necessity) with probable cause, simply because a computer was used as an instrumentality to commit a crime.

Conclusion that a computer search must be tailored with particularity with regard to the data contained on that machine.

85. Technology changed the world overnight. The former CEO of Apple, Inc., Steve Jobs, called the computer the "bicycle of the mind," referring to it as the greatest tool yet created by humans. And tracing the present growth of the nation's GDP suggests our society quickly realized this.

86. The vast majority of our existence and the new value created from our economy is now the result of information and intellectual property. The United States National Archives and Records Administration recently announced that a substantial majority of PACER will be made available for free, through the Internet, through the 125 person 503(c) non-profit called Wikipedia®, located in San Francisco, California. The IRS offers free software to assist in filing taxes because it results in more accurate tax-payer results and more people in the United States "e-file" their taxes than don't. Entire life histories that once were stored in photo albums are now stored digitally on hard drives and shared across the Internet, and they're filled with photos taken by "5.1 megapixel" cell phones. Even the President of the United States has a "Twitter® account" to publically announce messages on "social media," via the Internet. And all of this information and much more can be contained on a single personal computer no larger than a telephone book with a hard drive no larger than a New York Times® Bestseller® paperback novel.

87. The Sixth Circuit has clearly announced a standard recognizing this disparity between conventional items traditionally viewed as singular entities (e.g., a house or a filing cabinet) and computer storage because *computers hold a vast quantity of information unparalleled in our history.* While this Court is now aware *how information is stored* it is not aware of the sheer

quantity: twenty years ago, when I first used a computer, the amount of information that a personal computer could hold was nothing unparalleled to tangible analogies (e.g., the amount was similar to a filing cabinet – maybe even less). However, twenty years later, Silicon Valley has grown from a small, engineering industry in Santa Clara, California into numerous multiple billion-dollar technology companies packed inside the entire San Francisco Bay Area. The computer I'm now presently writing this on has about 5 terabytes of storage capacity which costed around $100. For comparison, researchers at Carnegie Mellon University, Princeton University, and Northwestern University, presently, believe that the human brain can store somewhere between 10-100 terabytes[18] to 2.5 petabytes[19]. Ex. 10. It is not enough to simply allow the search of a computer because it is an instrumentality in a crime because our privacy rights protect the digitalization of our lives.

88. Dorta made no attempt to limit his search *even to evidence of stalking*. Specifically, he searched, seized, and retains copies of "seven files...that appear to be files related to the, 'law closed' listserve As can be seen from the file paths that are listed beneath each file, these files were located in different parts of Enjaian's computer (from his gmail com account, form his Yahoo account, and from his upload folder from Dropbox." Ex. 18. Specifically, he searched, seized, and retains copies of "two...documents...extracted from the Chrome web browser cache under user Jesse in Enjaian's computer One shows the autofilled terms for his browser, while the

[18] "Tera" is a metric prefix that simply means a trillion of something and "peta" means 1,000 "tera." Hence, terabyte means a trillion bytes. Recall from above that each byte often represents a single letter. The present number of letters in this Complaint is only about 47,000 letters, or, in other words, 0.000000047% of one terabyte.

[19] Their estimations were based purely on a neural model of the human brain which is analogous to boolean storage of data making the comparison, here, meaningful.

other shows a history of keyword search terms from his browser." *Id*. Specifically, he searched, seized, and retains copies of "19 files that comprise...virtual machine[s]." *Id*. Specifically, he searched, seized, and retains copies of "two encrypted volumes found in Enjaian's computer Notice that one titles *[sic]*, 'work_files' was located in teh *[sic]* Documents directory for the user jesse The second encrypted volume titled mic tc wsa *[sic]* located under the directory Movies of the user Jesse." *Id*. Specifically, he searched, seized, and retains copies of "five images examined in this case." *Id*. U-M, presently, retains copies of all of this data. Undoubtedly, the *Richards* court would've referred to this wanton disregard for probable cause as "evidence of exploratory rummaging through files, or inadvertent discoveries." *Richards*, 659 F.3d at 542.

Claim VI: *Intentional infliction of emotional distress for the wrongful search and seizure against Dorta, under Michigan common law.*

89. Claim VI fully incorporates the contents and allegations of paragraphs 12-23 and *Claims I-II* and *IV-V*.

90. The willful delay and harassment described in *Claim IV*, and the willful search outside the scope of an objectively reasonable facial warrant described in *Claim V* all constitute extreme and outrageous conduct.

91. Dorta acted either maliciously, knowingly and intentionally, or recklessly as described in the references, incorporations, and incorporated claims.

92. At all times relevant to this Complaint, I was aware that Dorta was conducting his search only to delay and harass. Additionally, I became aware that Dorta exceeded the scope of the warrant simply to invade my privacy.

93. As a result of these facts and knowledge of these facts, I suffered severe emotional

distress including sleeplessness and anxiety.

Claim VII*: Defamation for malicious or intentional and knowing false statements imputing criminal conduct, against Schomp under MCL 600.2911 and Michigan common law.*

94. Claim VII fully incorporates the contents and allegations of paragraphs 12-23.

95. This claim is not barred by the statute of limitations because I did not discover the libelous email until approximately March, 2013 and the limitation was tolled while previously before this Court.

96. On March 27, 2012, Schomp maliciously or intentionally and knowingly submitted, via email, to both U-M and Dorta a letter containing various intentional and knowing false factual allegations ("Email"). Ex. 16. In other words, *Schomp criminally lied to the police*. I discovered the Email sometime in March, 2013 because this evidence was withheld from FOIA requests until then. I am alleging these conversations *never took place* and are complete, intentional *literary fiction*. A simple deposition of the mutual friend and ex-girlfriend, *infra*, can show that, contrary to Schomp's assertions in the Email, those conversations never took place. The Email contained the following false, factual assertions imputing criminal conduct against me:

97. Schomp asserted that a mutual friend's ("ND") parents instructed ND not to "go to the administration" about me because "they were afraid that if she did [I] could retaliate and harm her." *Id*. This conversation never took place nor did ND relay the asserted information to Schomp. Schomp fabricated this statement to impute that I assaulted ND or attempted battery.

98. Schomp asserted ND's then boyfriend (now husband) "was so confused and alarmed by the quick phone call [from ND], and evidently so concerned about his girlfriend's safety with

regard to [me] that he came over to her dorm room right away carrying a baseball bat." *Id*. This conversation never took place nor did this alleged physical altercation occur; nor is her husband a violent man nor, to the best of my knowledge and certainly my opinion, has he been. Schomp fabricated this statement to impute that I assaulted or battered ND or ND's then boyfriend.

99. Schomp asserted that my ex-girlfriend ("MM") told her "not to report the matter to the Law School administration" because I "would retaliate and you'll be sorry" and that MM would repeatedly state I am "probably fine he's a nice guy" as if MM "felt she was being recorded or had to cover her back." *Id*. My ex-girlfriend and I ended our relationship on a peaceful note and she never warned Schomp I would harm her for her malicious reports. Nor was she ever afraid I was somehow continually eavesdropping on her gossip while attending UMLS, and, according to the date of the Email, quite possibly in snow up to my chin. And it's hard to believe that Schomp's arm had to be twisted to complain about me. Schomp fabricated this statement to impute that I was criminally wiretapping MM or invading the privacy of MM.

100. Schomp asserted that MM told her that "she needed to be very careful" because I had "stalked her for a couple of weeks after [we] broke up" and that I would "pound on her door" and "wouldn't leave her alone." Schomp also asserted that MM told her "I don't know if [he has] a gun, but she would be worried he would shoot her" and that MM and her family "had been concerned by the fact that [I] and / or [my] family had a military background and had been concerned by this possibility." *Id*. My ex-girlfriend never accused me of stalking or even bothering her because we ended our relationship peacefully. Nor did my ex-girlfriend impute my possession of a firearm or intent to murder Schomp. Nor did my ex-girlfriend make bigoted and discriminatory statements against members and veterans of the United States military. Schomp

fabricated this statement to impute that I was criminally stalking MM and that I had, at least, attempted murder.

101. The assertion of these *per se* defamatory allegations as true to U-M and Dorta, via the Email, materially contributed to both the length of the seizure by Dorta and breadth and consequently the length and interference of the OSCR investigation which interfered with my schooling at UMLS.

102. The Email also caused interference, with my education at UMLS, from the then acting U-M Dean of Students because he extensively investigated and interviewed me in response to Schomp's false assertion that I was likely going to commit a mass-shooting at U-M and had already taken affirmative steps towards that goal.

103. The assertion of these *per se* defamatory allegations as true to U-M and Dorta, via the Email, caused reputation damage to me that includes future loss of earnings and the right to enjoyment of my livelihood. Additionally, I suffered emotional distress and pain and suffering, including loss of sleep and anxiety, as a result of the Email.

DAMAGES

104. As a result of Defendant Mundt's wrongful abuse of the warrant process, I suffered pain and suffering including loss of sleep and anxiety. The seizure occurred only several days prior to final examinations at UMLS, hence, it materially interfered with my education at UMLS. The 446 day seizure of my property is constructive conversion that required replacement of all equipment wrongfully seized. Additionally, I suffered public humiliation and loss of reputation for the false allegation of criminal stalking.

105. As a result of Defendant Dorta's wrongful search methodologies, my property was

searched for 446 days. The wrongful deprivation of my property caused pain and suffering including loss of sleep and anxiety. This seizure of my property is constructive conversion that required replacement of all equipment wrongfully searched.

106. As a result of Defendant Dorta's wrongful, overbroad search and seizure, intellectual property valued at over $10,000 was stolen from my computer. Additionally, the methods by which Dorta broke into my computer required over $10,000 to fix by implementing new cryptographic systems and programs and Internet-based archiving contracts, procedures, programs.

107. As a result of Defendant Schomp's libelous Email, both Dorta and a U-M employee believed the imputations of my criminal conduct contained in the Email. Additionally, both ND and MM were interviewed by UMLS, in response to the Email, harming my reputation with them and at U-M at-large. As a result of the lies purported as true in the Email, the University of Michigan Dean of Students conducted an investigation for the specific purpose of determining whether or not I intended to mass-murder students at U-M; this investigation caused pain and suffering including loss of sleep and anxiety.

JURY DEMAND

108. I respectfully demand a jury trial.

REQUESTED RELIEF

I respectfully request that:

109. This Court adjudge and decree that the warrant obtained by Mundt, in his official capacity, and used by U-M: (1) lacks probable cause and (2) is over broad.

110. This Court order Defendants Schlissel, Mundt, and Dorta to destroy all copies of

evidence seized from their illegal search and seizure of my property, and a compliance officer be appointed to supervise and certify the destruction.

111. I be awarded actual, nominal, and punitive damages in an amount to be determined at trial.

112. I be awarded costs with interest as provided in 42 U.S.C. § 1988, in MCL 600.2911, and under 18 U.S.C. § 1030.

113. I be awarded reasonable attorney fees as provided in MCL 600.2911 and under 18 U.S.C. § 1030; and all future counsel retained by me be awarded reasonable attorney fees under 42 U.S.C. § 1988 and in MCL 600.2911.

114. I be granted such further relief as this Court may deem just and proper.

October 14, 2014

Respectfully submitted,

/s/Jesse R. Enjaian
Jesse R. Enjaian
Pro se
4457 Alameda Drive
Fremont, CA 94536
(510) 793-0962
jenjaian@umich.edu

CERTIFICATE OF SERVICE

I hereby certify that on **October 14, 2014**, I electronically filed the foregoing paper with the Clerk of the Court using the ECF system which will send notification of such filing to the following: **Donica T. Varner**. I hereby certify that I have mailed by United States Postal Service the paper to the following non-ECF participants: **N/A**.

October 14, 2014

Respectfully submitted,

/s/Jesse R. Enjaian
Jesse R. Enjaian
Pro se
4457 Alameda Drive
Fremont, CA 94536
(510) 793-0962
jenjaian@umich.edu